PTO/SB/21 (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Applicati n Number	10/605,540
Filing Date	10/07/2003
First Named Inventor	Chih-Pen Chang
Group Art Unit	
Examiner Name	
Total Number of Pages in This Submission: 3	Attorney Docket Number: ALIP0015USA

ENCLOSURES *(check all that apply)*

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment / Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [x] Certified Copy of Priority Document(s)
- [ ] Response to Missing Parts/ Incomplete Application
  - [ ] Response to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Assignment Papers *(for an Application)*
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
- [ ] After Allowance Communication to Group
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to Group *(Appeal Notice, Brief, Reply Brief)*
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) *(please identify below)*:

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Winston Hsu, Reg. No.: 41,526
Signature	Winston Hsu
Date	10/28/2003

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, Washington, DC 20231 on this date: _____

Typed or printed name			
Signature		Date	

PTO/SB/17 (01-03)
Approved for use through 04/30/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

FEE TRANSMITTAL for FY 2003

Effective 01/01/2003. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 0.00

Complet if Known	
Application Number	10/605,479
Filing Date	10/07/2003
First Named Inventor	Chih-Pen Chang
Examiner Name	
Art Unit	
Attorney Docket No.	ALIP0015USA

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☑ Deposit Account:

Deposit Account Number: 50-0801

Deposit Account Name: North America International Patent Office

The Commissioner is authorized to: *(check all that apply)*

☑ Charge fee(s) indicated below ☑ Credit any overpayments

☑ Charge any additional fee(s) during the pendency of this application

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	750	2001	375	Utility filing fee	
1002	330	2002	165	Design filing fee	
1003	520	2003	260	Plant filing fee	
1004	750	2004	375	Reissue filing fee	
1005	160	2005	80	Provisional filing fee	

SUBTOTAL (1) ($) 0.00

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims		Fee from below	Fee Paid
Total Claims		-20** =		X	=
Independent Claims		- 3** =		X	=
Multiple Dependent					=

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	18	2202	9	Claims in excess of 20
1201	84	2201	42	Independent claims in excess of 3
1203	280	2203	140	Multiple dependent claim, if not paid
1204	84	2204	42	** Reissue independent claims over original patent
1205	18	2205	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	110	2251	55	Extension for reply within first month	
1252	410	2252	205	Extension for reply within second month	
1253	930	2253	465	Extension for reply within third month	
1254	1,450	2254	725	Extension for reply within fourth month	
1255	1,970	2255	985	Extension for reply within fifth month	
1401	320	2401	160	Notice of Appeal	
1402	320	2402	160	Filing a brief in support of an appeal	
1403	280	2403	140	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	110	2452	55	Petition to revive - unavoidable	
1453	1,300	2453	650	Petition to revive - unintentional	
1501	1,300	2501	650	Utility issue fee (or reissue)	
1502	470	2502	235	Design issue fee	
1503	630	2503	315	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	750	2809	375	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	750	2810	375	For each additional invention to be examined (37 CFR 1.129(b))	
1801	750	2801	375	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid **SUBTOTAL (3)** ($) 0.00

SUBMITTED BY				(Complete *(if applicable)*)	
Name (Print/Type)	Winston Hsu	*Registration No. (Attorney/Agent)*	41,526	*Telephone*	886289237350
Signature	Winston Hsu	*Date*	10/28/2003		

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

This collection of information is required by 37 CFR 1.17 and 1.27. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, Washington, DC 20231.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

PTO/SB/02B (11-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

DECLARATION — Supplemental Priority Data Sheet

Additional foreign applications:

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached? YES	NO
092105706	Taiwan R.O.C	03/14/2003	☐	☑	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder：

申　　請　　日 ： 西元 2003 年 03 月 14 日
Application Date

申　請　案　號 ： 092105706
Application No.

申　　請　　人 ： 揚智科技股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元 2003 年 9 月 25 日
Issue Date

發文字號： 09220963230
Serial No.

申請日期：	IPC分類
申請案號：	

(以上各欄由本局填註)

發明專利說明書

一、發明名稱	中文	具有一反向密鑰推導電路之加解密系統
	英文	CRYPTO-SYSTEM WITH AN INVERSE KEY EVALUATION CIRCUIT
二、發明人(共2人)	姓名(中文)	1.張志鵬 2.賴明祥
	姓名(英文)	1.Chang, Chih-Pen 2.Lai, Ming-Shiang
	國籍(中英文)	1.中華民國 TW 2.中華民國 TW
	住居所(中文)	1.台北縣板橋市漢生東路二七九巷十弄十六之二號 2.新竹市東南街二八七號
	住居所(英文)	1.No. 16-2, Alley 10, Lane 279, Han-Sheng E. Rd., Pan-Chiao City, Taipei Hsien, Taiwan, R.O.C. 2.No. 287, Tung-Nan St., Hsin-Chu City, Taiwan, R.O.C.
三、甲請人(共1人)	名稱或姓名(中文)	1.揚智科技股份有限公司
	名稱或姓名(英文)	1.Acer Laboratories, Inc.
	國籍(中英文)	1.中華民國 TW
	住居所(營業所)(中文)	1.台北縣汐止市新台五路一段88號21樓　(本地址與前向貴局申請者相同)
	住居所(營業所)(英文)	1.21F, No. 88, Sec.1, Hsin-Tai Wu Rd., Hsi-Chih City, Taipei Hsien, Taiwan, R.O.C.
	代表人(中文)	1.呂理達
	代表人(英文)	1.Lu, Teddy

四、中文發明摘要　（發明名稱：具有一反向密鑰推導電路之加解密系統）

本發明提供一反向密鑰推導電路及具有該反向密鑰推導電路之加解密系統，該反向密鑰推導電路包含有一密鑰接收模組以及一反向密鑰推導模組，密鑰接收模組包含一位元暫存器，用來接收及儲存一密鑰。反向密鑰推導模組用來將該密鑰接收模組所接收的密鑰經過複數次反向推導處理後依序分別產生該密鑰之複數個前級密鑰，而儲存於該位元暫存器中的密鑰會依序被由該密鑰所產生的前級密鑰所取代。該加解密系統包含有一具有該反向密鑰推導模組之密鑰產生模組、一加密模組、以及一解密模組。

代表圖（一）、本案代表圖為：第　5　圖

（二）、本案代表圖之元件代表符號簡單說明

60　加解密系統　　62　密鑰產生模組

64　加密模組　　65　加密電路

六、英文發明摘要　（發明名稱：CRYPTO-SYSTEM WITH AN INVERSE KEY EVALUATION CIRCUIT）

An inverse key evaluation circuit for inversely generating a plurality of pre-keys in sequence according to an original key and a crypto-system containing the inverse key evaluation circuit for decrypting a ciphered text into a plain text according to the plurality of pre-keys. The inverse key evaluation circuit includes a key-receiving module and an inverse key

四、中文發明摘要　(發明名稱：具有一反向密鑰推導電路之加解密系統)

66　解密模組　　70　正向密鑰推導電路
72　反向密鑰推導電路　　74　唯讀記憶體
78　位元暫存器　　82　密鑰增生層
84　位元組替代層　　86　列偏移層
88　行混排層

六、英文發明摘要　(發明名稱：CRYPTO-SYSTEM WITH AN INVERSE KEY EVALUATION CIRCUIT)

evaluation module. The key-receiving module includes a register for temporally receiving and storing the original key, which will be processed by the inverse key evaluation module to generate the plurality of pre-keys of the original key, and the key stored in the register will be replaced by the newly generated pre-key in sequence. The crypto-system includes a

四、中文發明摘要　（發明名稱：具有一反向密鑰推導電路之加解密系統）

六、英文發明摘要　（發明名稱：CRYPTO-SYSTEM WITH AN INVERSE KEY EVALUATION CIRCUIT）

key-generating module that contains the inverse key evaluation circuit, an encryption module, and a decryption module.

一、本案已向

國家(地區)申請專利	申請日期	案號	主張專利法第二十四條第一項優先

無

二、□主張專利法第二十五條之一第一項優先權:

申請案號:

無

日期:

三、主張本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間

日期:

四、□有關微生物已寄存於國外:

寄存國家:

寄存機構: 無

寄存日期:

寄存號碼:

□有關微生物已寄存於國內(本局所指定之寄存機構):

寄存機構:

寄存日期: 無

寄存號碼:

□熟習該項技術者易於獲得,不須寄存。

五、發明說明 (1)

發明所屬之技術領域：

本發明提供一種加解密系統，尤指一種具有一反向密鑰推導電路之加解密系統及相關之解密方法，來減少隨機存取記憶體的使用。

先前技術

無線區域網路(wireless LAN)與一般固定式區域網路的最大差異在於無線區域網路是利用無線電波來傳輸資料，而後者則大多是利用電纜線或光纖來傳遞，而由於無線電波較容易受到攔截，因此資料安全性對於無線區域網路成為更重要的課題，如IEEE所提出的802.11i即是為了加強無線網路資料的安全所制定的一個標準。事實上，使用密碼學技術以期對網路提供最佳的安全防禦的概念適用於各式各樣的網路傳輸，其中最著名也最普遍使用的密碼系統為使用56位元密鑰的資料加密標準(Data Encryption Standard, DES)，但隨著電子科技的發展與電腦運算速度的提升，設計破解資料加密標準的特殊硬體或以多部電腦合作破解資料加密標準的構想與實驗近幾年來一再被提出，這也使得以資料加密標準為密碼演算法機制的系統安全性堪虞，而2000年10月美國政府機構NIST正式宣布選用Rijndael演算法作為新的規格--先進加密標準(Advanced Encryption Standard,

AES)，且於2001年成為美國聯邦資訊處理加密標準，以逐步取代早期的資料加密標準，關於Rijndael演算法及以其為基礎之先進加密標準請見J. Daemen及V. Rijmen於2001年於Dr. Dobb's Journal發表之 "Rijndael, the advanced encryption standard''等文獻。

先進加密標準AES是一個區塊加密/解密(block cipher/deciper)的演算法，它在實現IEEE 802.11i標準中的網路安全裏，扮演極重要的一個基礎角色，所有的安全模式皆以先進加密標準演算法為基礎，再加以延伸應用。先進加密標準在依密鑰類型不同區分的現代密碼技術中可歸類為對稱加密系統，也就是加密和解密都奠基於同一把密鑰。由於對稱加密系統本身的性質，對稱加密系統的安全性主要依賴以下兩個因素，第一，加密算法必須夠強大，讓僅依加密後的密文本身去得到解密信息在實踐上是不可能的；第二，加密的安全性主要依賴密鑰的秘密性，而不是加/解密演算法的隱密性，因此，密鑰秘密性的確保變得更為重要。在Liu等人提出的US Patent No. 5,539,827, "Device and method for data encryption"中，使用者可利用一密鑰自訂加/解密時的加密強度(encryption intensity)，並增加加密過程的秘密性，而在Coppersmith等人提出的US Patent No. 6,192,129, "Method and apparatus for advanced byte-oriented symmetric key block cipher with

variable length key and block"及同一組發明者隨後提出之 US Patent No. 6,243,470, "Method and apparatus for advanced symmetric key block cipher with variable length key and block"中，亦揭露了類似先進加密標準的加/解密演算法，並利用可讓使用者自訂可變動長度的密鑰，增加加密過程的複雜度。

先進加密標準的明文固定為128位元，密鑰則亦可訂為128位元。請參閱圖一，圖一為符合先進加密標準之一習知加解密系統10運作的功能方塊圖。如圖所示，先進加密標準每回合是由四個可逆的轉換層所組成，包括一密鑰增生層 (KeyAddition)12、一位元組替代層(ByteSubstitution)14、一列偏移層 (ShiftRow)16、以及一行混排層 (MixColumn)18，一控制模組20可用來控制每回合的循環演算 (round evaluation)，經過四個轉換層的循環演算總共會反覆10次，每次皆需要不同的密鑰，這些不同的密鑰即是經由一密鑰排程模組22(key scheduling)所產生，並藉由這些不同的密鑰來增加編碼資料的亂度。因此，我們實現的128位元密鑰之先進加密標準的加密過程即如圖一所示：一128位元(加解密)密鑰(此為最初之密鑰，可稱為母鑰)先經過密鑰排程模組22予以擴張計算出接下來另10組128位元的密鑰，每次產生出來的密鑰即用來用於當次之循環演算，將文件作一次的加/解密運作，此種運作根據包含母鑰之11組128位元

的密鑰將文件作11次的加/解密運作。

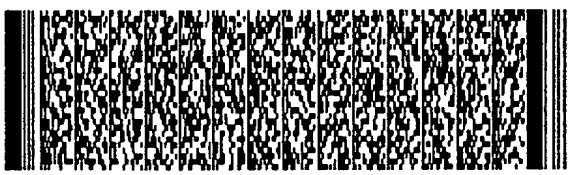
以硬體來實現先進加密標準時，在密鑰安排模組中會執行一重要的密鑰排程演算法(Key scheduling algorithm)，如前所述，它的目的在於將上層給的密鑰，在先進加密標準之每回合循環演算時，提供一個跟上一級密鑰完全不相同的密鑰，目的在於產生一堆彼此不相同，但確有相關性的密鑰，以確保以此密鑰為基礎的加密方法，可以讓加密出來的資料與原本資料有最大的差異性。請繼續參閱圖一，先進加密標準之架構另包含一唯讀記憶體(ROM)24，來儲存對應於該複數個加密解操作之演算法及相關之應用程式，另外，傳統習知技術必需利用到一可供暫時性運算變數資料儲存用的隨機存取記憶體(Random Access Memory, RAM) 26來儲存所有推算出來的密鑰，然後在每次循環演算時，抓取要用的密鑰，首先，在評估演算法效率時，越大的程式及表格(佔用唯讀記憶體24區域越大)或越多推算出來的密鑰等的暫時變數(使用隨機存取記憶體26區域越大)通常可加快執行速度，但同時亦增加記憶體所佔的空間和成本，由上所述，此隨機存取記憶體26必須要儲存包含有母鑰之11組128位元的密鑰，會佔去相當的空間和成本，此外，儲存有越多推算出來的密鑰的隨機存取記憶體26亦會造成接收器在存取資料上時間的延遲，而導致效能的降低。

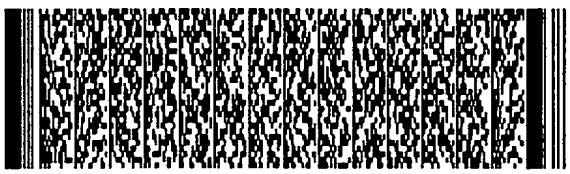
發明內容

因此本發明的主要目的在於一種具有一反向密鑰推導電路之加解密系統及相關方法，來減少記憶體的使用，以解決上述問題。

在本發明中，我們首先提出一種用於一加解密系統中的反向密鑰推導電路以及相關之解密方法，以減少隨機存取記憶體的使用亦不造成接收器在存取資料上的延遲，接下來本發明之加解密系統將加密(encryption)與解密(decryption)分成兩個不同的模組完成，加密採用一唯讀記憶體式(ROM-based)的方式來加快計算速度，解密的部份利用反向密鑰推導電路以及相關解密法，而本發明之加解密系統之加密與解密部分共用一個密鑰產生模組，使電路運算的速度不減少，亦不必增加其他額外的電路，即完成先進加密標準之硬體實現。

本發明之申請專利範圍提供一種用於一加解密系統中的反向密鑰推導電路(Inverse Key Evaluation Circuit)，其包含有一密鑰接收模組，其包含一N位元暫存器，該N位元暫存器包含有m組位元暫存器，用來接收一N位元之密鑰，該N位元之密鑰包含有m群密鑰，該m群密鑰係分別儲存於該m組位元暫存器中，其中N及m係為2

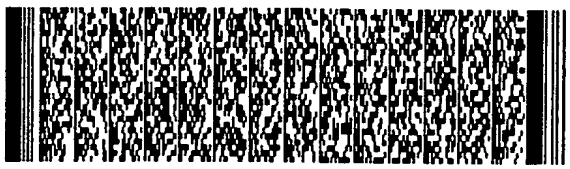




的乘冪且大於2之整數；以及一反向密鑰推導模組，其包含m個互斥或(XOR)邏輯閘以及一數位資料處理模組，用來將該密鑰接收模組所接收的密鑰經過複數次反向推導處理後，依序分別產生該密鑰相對應之複數個前級密鑰；其中儲存於該N位元暫存器中的密鑰會依序被由該密鑰經一次該反向密鑰推導模組處理後所得出的前一級密鑰所取代。

本發明之申請專利範圍另提供一種解密方法，用來將一N位元之密文字串解密為一對應之N位元之明文字串，其中N係為一2的乘冪且大於2之整數；該解密方法包含有：提供一密鑰與該密文字串；使用一反向密鑰推導模組，依序產生該密鑰之複數個前級密鑰；以及依序使用該密鑰以及由該密鑰所產生之複數個前級密鑰，配合複數個相對應的解密操作(Decryption Operation)，將該密文字串解密為該明文字串。

本發明之申請專利範圍又提供一種加解密系統，用來執行複數個加密操作以及複數個解密操作，該加解密系統包含有一密鑰產生模組，用來提供複數個密鑰，該密鑰產生系統包含有一正向密鑰推導電路，用來依據一母鑰，依序產生該母鑰之複數個後級密鑰至一最後級密鑰為止；一反向密鑰推導電路，用來依據該最後級密鑰，依序產生該最後級密鑰之複數個前級密鑰至該母鑰



為止；以及至少一位元暫存器，用來儲存該母鑰以及該最後級密鑰；一加密模組，電連於該密鑰產生模組，用來依據該正向密鑰推導電路所提供之母鑰及依序產生之複數個後級密鑰，依序執行相對應之複數個加密操作，將一明文字串加密為一對應之密文字串；以及一解密模組，電連於該密鑰產生模組，用來依據該反向密鑰推導電路所提供之最後級密鑰及依序產生之複數個前級密鑰，依序執行相對應之複數個解密操作，將一密文字串解密為一對應之明文字串。

實施方式

本發明之技術特徵係奠基於一先進加密標準（AES）上，並以最佳效能來完成以硬體來實現先進加密標準的目標。在本發明中，我們首先揭露一種反向密鑰推導電路（Inverse Key Evaluation Circuit），可用來擴充推導出一密鑰之複數個相關之前級密鑰並以之減少隨機存取記憶體的使用。承襲部分圖一習知技術在實現先進加密標準上的技術特徵，於一加解密系統中，用於加密之一密鑰（此為最初之密鑰，可稱為母鑰）先予以擴張計算出接下來另10組的後級密鑰，而在解密時，所需要密鑰的順序與加密時的密鑰順序完全是相反的，也就是說，如果加密的密鑰經由推導後的順序是密鑰0(母鑰)、密鑰1、密鑰2、密鑰3……密鑰10，則解密所需的密鑰順序

就是密鑰10、密鑰9、密鑰8……..密鑰1、密鑰0(母鑰)。

請參閱圖二，圖二為本發明反向密鑰推導電路32之一實施例之功能方塊圖。反向密鑰推導電路32包含有一密鑰接收模組34以及一反向密鑰推導模組36，密鑰接收模組34包含一N位元暫存器38，N位元暫存器38包含有m組位元暫存器38，用來接收一N位元之密鑰，而此N位元之密鑰又可分成m群密鑰，此m群密鑰係分別儲存於m組位元暫存器38中，其中N及m係為2的乘冪且大於2之整數，而在本實施例中，由於先進加密標準的規範，N值係為128，而m的值則因演算法之故設為4，在實際實施時可再依實際情況調整N及m的數值。反向密鑰推導模組36包含有m個互斥或(XOR)邏輯閘40，其中互斥或邏輯閘40的數目是對應於密鑰的群數，用來將此m群密鑰兩兩作相關的互斥或(XOR)運算處理。反向密鑰推導模組36另包含一數位資料處理模組42，電連於此m個互斥或邏輯閘40後，用來將密鑰接收模組34所接收的密鑰經過複數次反向推導處理後，依序分別產生與此密鑰相對應之複數個前級密鑰，而整個過程和前述習知技術相同，會重複運作10次，以依序產生該密鑰之10個前級密鑰，亦即此128位元之密鑰即可稱為密鑰10，該密鑰之10個前級密鑰也就是密鑰9至密鑰0。請注意，儲存於密鑰接收模組34之N位元暫存器38中的密鑰會依序被由此密鑰經一次反向密鑰推

導模組36處理後所得出的前一級密鑰所取代，也就是說，利用本發明反向密鑰推導電路32之技術特徵，只需要一N位元暫存器38，亦即128位元的位元暫存器，去儲存產生出來的密鑰(在實際實施時位元暫存器可以隨機存取記憶體完成)，相較於習知技術中，因為沒有類似的密鑰反向推導的機制，因此隨機存取記憶體必須要儲存包含有母鑰及所有由其產生之密鑰(共11組128位元的密鑰)相比，本發明之反向密鑰推導電路大幅降低記憶體電路之空間和成本。

請參閱圖三，圖三為圖二反向密鑰推導電路32之一詳細實施例之功能方塊圖。電連於4個互斥或邏輯閘40後的數位資料處理模組42包含有一位元組反轉器(Byte Rotator)43、一位元組取代器(Byte Substitute)45、以及一位元組混排器(Byte Disturber)47。位元組反轉器43用來將傳送來之密鑰中之複數個位元組順序反轉，位元組取代器45則電連於位元組反轉器43，用來將密鑰中的複數個位元組以複數個預設位元組替代，而位元組混排器47則依據一預設混排表來產生一混排值，與密鑰中的複數個位元組做互斥或運算。經過一次反向密鑰推導電路32中之4個互斥或邏輯閘40及數位資料處理模組42處理後所得出的前一級密鑰會儲存於此實施例中新包含的一位元暫存器48，其電連於反向密鑰推導模組36後，與圖二及圖三中密鑰接收模組34之128位元暫存器38的運作

同理，儲存於位元暫存器48之密鑰會被由該密鑰經一次反向推導處理後所產生的前一級密鑰所取代，因此位元暫存器48亦只需128位元來儲存密鑰。由於在本實施例包含了兩組位元暫存器，即在密鑰接收模組34之128位元暫存器38之外又另外設置的位元暫存器48，因此經一次反向推導處理後所產生的前一級密鑰會先儲存於另外設置的位元暫存器48，因此需要一密鑰更新器50，連接於密鑰接收模組34之128位元暫存器38及另設置的位元暫存器48之間，於收到一密鑰更新訊號後，將新得到的前級密鑰覆寫至密鑰接收模組34之128位元暫存器38。

由於本發明實施例之反向密鑰推導電路32之原理仍是奠基於先進加密標準(AES)上，因此本發明之反向密鑰推導電路32係可應用於一無線區域網路(Wireless LAN)中，且上述之反向密鑰推導電路32是應用在一解密相關之方法及裝置中。請見圖四，圖四為本發明根據圖二及圖三實施例之一解密方法的流程圖。本發明解密方法是用來將一N位元之密文字串解密為一對應之N位元之明文字串，N為一2的乘冪且大於2之整數，根據圖二及圖三實施例，N之值為128，意即密文字串及明文字串皆為128位元之數位資料，而在根據先進加密標準實際實施時，密鑰亦設成128位元。解密方法包含的步驟如下：

步驟100：提供一密鑰與密文字串；

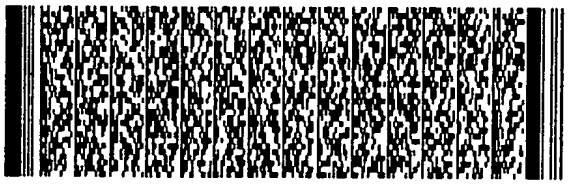
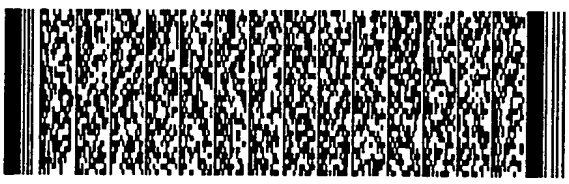
步驟101：使用一反向密鑰推導模組36，依序產生該密鑰之複數個前級密鑰；

步驟102：使用一位元暫存器48，依序儲存該密鑰及其所產生之複數個前級密鑰；

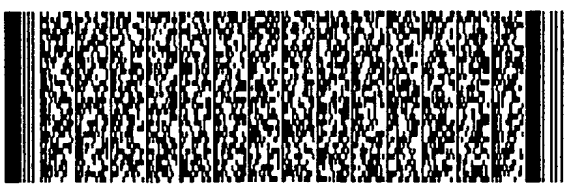
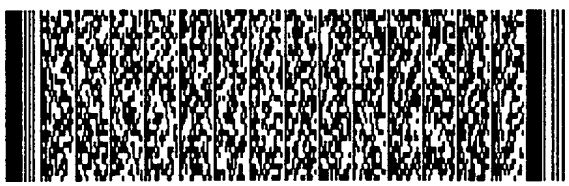
步驟103：依序使用該密鑰以及由其所產生之複數個前級密鑰，配合複數個相對應的解密操作(Decryption Operation)，將密文字串解密為明文字串。

在步驟102中，儲存於位元暫存器48中的密鑰會依序被由該密鑰經一次反向密鑰推導模組36處理後所產生的前一級密鑰所取代，因此位元暫存器48亦只需128位元來儲存密鑰，而亦無須如習知技術之記憶體般必須要儲存所有由該密鑰所產生之複數個(連最初之密鑰共11個)128位元的密鑰。

上述所有的實施例及方法都依據本發明反向密鑰推導電路32所揭露之技術特徵，也就是利用一「最後一級密鑰」推導出其複數個前級密鑰，如前所述，在實現先進加密標準上的技術特徵時，用於加密之一128位元密鑰(此為最初之密鑰，可稱為母鑰)先經過反向密鑰推導電路32予以擴張計算出接下來另10組的後級密鑰，而在解密時，所需要密鑰的順序與加密時的密鑰順序完全是相反的，而無須將所有的密鑰儲存下來，只需儲存最後一級密鑰便可推導出其複數個前級密鑰，這便是反向密鑰

推導電路32最重要的功能。採用此反向密鑰推導電路32之完整的一加解密系統請見圖五，圖五為本發明加解密系統60之功能方塊圖。加解密系統60包含有一密鑰產生模組62、一加密模組64、以及一解密模組66。密鑰產生模組62可用來推導產生加/解密所需之複數個密鑰，並判斷當下為加密模組64或解密模組66在運作而傳送相對應的密鑰。密鑰產生模組62又包含有一正向密鑰推導電路70、一反向密鑰推導電路72(對應於圖二及圖三實施例之反向密鑰推導電路32)、以及一位元暫存器78。正向密鑰推導電路70可依據一母鑰，依序產生該母鑰之複數個後繼密鑰至一最後級密鑰為止，反向密鑰推導電路72則可依據最後級密鑰，依序產生最後級密鑰之複數個前級密鑰至母鑰為止。依據先進加密標準，可設正向密鑰推導電路70由母鑰所推導後的順序為：密鑰0(母鑰)、密鑰1、密鑰2、密鑰3……密鑰10，而反向密鑰推導電路72推導出解密所需的密鑰順序就是密鑰10、密鑰9、密鑰8……密鑰1、密鑰0(母鑰)，另外密鑰產生模組62中之位元暫存器78可用來儲存該母鑰(密鑰0)以及該最後級密鑰(密鑰10)，當加密模組64要將一明文字串加密為密文字串時，正向密鑰推導電路70就會將儲存於位元暫存器78中的母鑰(密鑰0)及依據其產生之複數個後級密鑰(密鑰1至密鑰10)依序提供予加密模組64，同時，位元暫存器78也會存入最後級密鑰(密鑰10)以供解密模組66將密文字串解密。位元暫存器78必須先存入最後級密鑰(密鑰

10)的原因在於資料在接收時，並沒有額外的時間可以讓正向密鑰推導電路70去推算出最後級密鑰(密鑰10)，然後再反推解密所需要的密鑰，所以必須利用加密的同時，先將推算出最後級密鑰(密鑰10)存入位元暫存器78中，等待需要解密時，直接利用存於位元暫存器78中的最後級密鑰(密鑰10)供反向密鑰推導電路72處理。加密模組64包含一電連於密鑰產生模組62的加密電路65，用來依據正向密鑰推導電路70所提供之母鑰(密鑰0)及依序產生之複數個後級密鑰(密鑰1至密鑰10)，依序執行相對應之複數個加密操作，將一明文字串加密為一對應之密文字串，這些加密操作近似於圖一習知技術所述之複數回合之循環演算，但包含有加密電路65的加密模組64於此實施例中為一改良後之唯讀記憶體式(ROM-based)加密模組64，包含有複數個唯讀記憶體74來儲存對應於複數個加密操作之演算法及相關之應用程式，可取代於圖一中四個可逆的轉換層中的部分功能，以唯讀記憶體74中儲存的程式及表格更迅速地完成。解密模組66亦電連於密鑰產生模組62，用來依據反向密鑰推導電路72所提供之最後級密鑰(密鑰10)及依序產生之複數個前級密鑰(密鑰9至密鑰0)，依序執行相對應之複數個解密操作，將一密文字串解密為一對應之明文字串，這些解密操作則沿用圖一習知技術所述之複數回合用以解密之循環演算的架構，意即包含了密鑰增生層82、位元組替代層84、一列偏移層86、以及一行混排層88來執行相對應之解密操

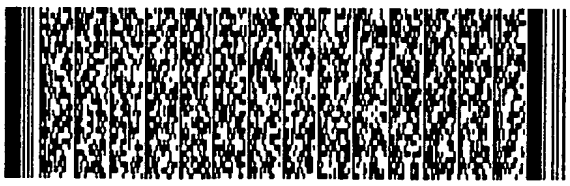
作，將一密文字串轉換為原先對應之明文字串。

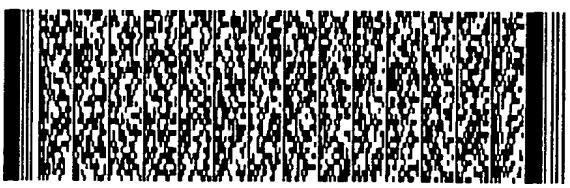
請注意，首先，本實施例中密鑰產生模組62之正向密鑰推導電路70可以大致近似於圖一習知技術所描述之密鑰排程模組22，另外，本實施例之位元暫存器78只需要儲存母鑰(密鑰0)以及最後級密鑰(密鑰10)二個密鑰，甚至位元暫存器78只需要儲存母鑰(密鑰0)即可，但此時於反向密鑰推導電路72中必須再包含一位元暫存器，用來儲存解密所需之最後級密鑰(密鑰10)，無論何種設置法，都大幅降低習知技術中記憶體用來儲存所有密鑰(密鑰0至密鑰10)所佔的記憶空間。請見圖六，圖六為圖五反向密鑰推導電路72之一實施例，本實施例近似於圖二之實施例，仍包含有一密鑰更新器90、一密鑰接收模組94、一反向密鑰推導模組96、以及一位元暫存器98。密鑰接收模組94用來接收並儲存最後級密鑰(密鑰10)，反向密鑰推導模組96用來將密鑰接收模組94所接收的最後級密鑰(密鑰10)經過複數次反向推導處理後，依序產生最後級密鑰之複數個前級密鑰至母鑰為止(密鑰9至密鑰0)，而位元暫存器98電連於反向密鑰推導模組96後，用來儲存一經一次反向推導處理後所得出的前級密鑰，同樣儲存於位元暫存器98之密鑰會被由該密鑰經一次反向推導處理後所產生的前一級密鑰所取代。當整個圖五之加解密系統60初始啟動(System Reset)或汰換舊的母鑰(密鑰0)成新的母鑰時，便有一初始化的流程將母鑰(密

鑰 0)推算至最後級密鑰(密鑰 10)(該初始化流程可由圖五之正向密鑰推導電路 70完成),同時密鑰更新器 50會收到一密鑰更新訊號並將新的最後級密鑰(密鑰 10)接收進密鑰接收模組 94中,當然之後密鑰更新器 50亦能將經一次反向推導處理後產生的前級密鑰由位元暫存器 98再覆寫至密鑰接收模組 94中。

本發明之加解密系統將加密(encryption)與解密(decryption)分成兩個不同的模組完成,加密採用一唯讀記憶體式(ROM-based)的方式來加快計算速度,解密的部份利用一反向密鑰推導電路以及相關解密法,可依序逆向推算前級的密鑰,並只需用少量的記憶體儲存一初始及最後級之密鑰,使得此加解密系統可減少隨機存取記憶體的使用亦不造成接收器在存取資料上的延遲,再者本發明之加解密系統之加密與解密部分共用一個密鑰產生模組,使電路運算的速度不減少,亦不必增加其他額外的電路,即完成先進加密標準之硬體實現。

以上所述僅為本發明之較佳實施例,凡依本發明申請專利範圍所做之均等變化與修飾,皆應屬本發明專利之涵蓋範圍。





圖式之簡單說明

圖一為習知符合先進加密標準之一加解密系統的功能方塊圖。

圖二為本發明反向密鑰推導電路之一實施例的功能方塊圖。

圖三為圖二反向密鑰推導電路之一實施例的功能方塊圖。

圖四為本發明之一解密方法的流程圖。

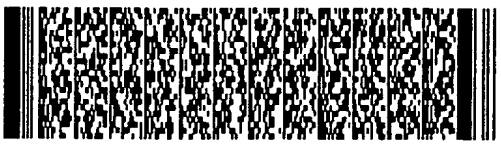
圖五為本發明一加解密系統之功能方塊圖。

圖六為圖五反向密鑰推導電路之一實施例的功能方塊圖。

圖式之符號說明

10、60	加解密系統	12、82	密鑰增生層
14、84	位元組替代層	16、86	列偏移層
18、88	行混排層	20	控制模組
22	密鑰排程模組	24、74	唯讀記憶體
26	隨機存取記憶體		
32、72	反向密鑰推導電路		
34、94	密鑰接收模組		
36、96	反向密鑰推導模組		
38、48、78、98	位元暫存器		

40	互斥或邏輯閘		
42	數位資料處理模組		
43	位元組反轉器		
45	位元組取代器	47	位元組取代器
50、90	密鑰更新器	62	密鑰產生模組
64	加密模組	65	加密電路
66	解密模組		
70	正向密鑰推導電路		



六、申請專利範圍

1. 一種用於一加解密系統中的反向密鑰推導電路(Inverse Key Evaluation Circuit)，其包含有：

一密鑰接收模組，其包含一N位元暫存器，該N位元暫存器包含有m組位元暫存器，用來接收一N位元之密鑰，該N位元之密鑰包含有m群密鑰，該m群密鑰係分別儲存於該m組位元暫存器中，其中N及m係為2的乘冪且大於2之整數；以及

一反向密鑰推導模組，其包含m個互斥或(XOR)邏輯閘以及一數位資料處理模組，用來將該密鑰接收模組所接收的密鑰經過複數次反向推導處理後，依序分別產生該密鑰相對應之複數個前級密鑰；

其中儲存於該N位元暫存器中的密鑰會依序被由該密鑰經一次該反向密鑰推導模組處理後所得出的前一級密鑰所取代。

2. 如申請專利範圍第1項之反向密鑰推導電路，其中N及m的值係分別為128以及4，並且最初由該密鑰接收模組所接收的密鑰可分別經過10次反向推導處理後，依序產生該密鑰之10個前級密鑰。

3. 如申請專利範圍第1項之反向密鑰推導電路，其中該反向密鑰推導模組中之數位資料處理模組係電連於該m個互斥或邏輯閘後，該數位資料處理模組包含有：

一位元組反轉器(Byte Rotator)，用來將該N位元之

密鑰中之複數個位元組順序反轉；

一位元組取代器(Byte Substitute)，電連於該位元組反轉器，用來將該N位元之密鑰中的複數個位元組以複數個預設位元組替代；以及

一位元組混排器(Byte Disturber)，依據一預設混排表來產生一混排值，與該N位元之密鑰中的複數個位元組做互斥或運算。

4. 如申請專利範圍第1項之反向密鑰推導電路，其另包含一位元暫存器，電連於該反向密鑰推導模組，用來儲存一經一次該反向推導處理後所產生的密鑰，其中儲存於該位元暫存器之密鑰會被由該密鑰經一次反向推導處理後所產生的前一級密鑰所取代。

5. 如申請專利範圍第1項之反向密鑰推導電路，其中該加解密系統係符合一先進加密標準(Advanced Encryption Standard, AES)。

6. 如申請專利範圍第5項之反向密鑰推導電路，其中該加解密系統係應用於一無線區域網路(Wireless LAN)上。

7. 一種解密方法，用來將一N位元之密文字串解密為一對應之N位元之明文字串，其中N係為一2的乘冪且大於2

之整數；

該解密方法包含有：

提供一密鑰與該密文字串；

使用一反向密鑰推導模組，依序產生該密鑰之複數個前級密鑰；以及

依序使用該密鑰以及由該密鑰所產生之複數個前級密鑰，配合複數個相對應的解密操作(Decryption Operation)，將該密文字串解密為該明文字串。

8. 如申請專利範圍第7項所述之方法，其另包含有使用一位元暫存器，依序儲存該密鑰及該密鑰所產生之複數個前級密鑰，其中儲存於該位元暫存器中的密鑰會依序被由該密鑰經一次該反向密鑰推導模組處理後所產生的前一級密鑰所取代。

9. 如申請專利範圍第7項所述之方法，其中該密鑰係為一N位元之密鑰，N的值係為128，且該密鑰係可經由該反向密鑰推導模組，依序產生該密鑰之10個前級密鑰。

10. 如申請專利範圍第9項所述之方法，其中該反向密鑰推導模組包含有m個互斥或(XOR)邏輯閘以及一數位資料處理模組，用來將該密鑰經過複數次反向推導處理後，依序分別得出該密鑰相對應之複數個前級密鑰，其中m係為一2的乘冪且大於2之整數。

11. 如申請專利範圍第10項所述之方法，其中該數位資料處理模組係電連於該m個互斥或邏輯閘後，該數位資料處理模組包含有：

一位元組反轉器(Byte Rotator)，用來將該N位元之密鑰中之複數個位元組順序反轉；

一位元組取代器(Byte Substitute)，電連於該位元組反轉器，用來將該N位元之密鑰中的複數個位元組以複數個預設位元組替代；以及

一位元組混排器(Byte Disturber)，依據一預設混排表來產生一混排值，與該N位元之密鑰中的複數個位元組做互斥或閘運算。

12. 如申請專利範圍第7項所述之方法，其係符合一先進加密標準(Advanced Encryption Standard, AES)。

13. 如申請專利範圍第12項所述之方法，其係應用於一無線區域網路(Wireless LAN)之一加解密系統上。

14. 一加解密系統，用來執行複數個加密操作以及複數個解密操作，該加解密系統包含有：

一密鑰產生模組，用來提供複數個密鑰，該密鑰產生模組包含有：

六、申請專利範圍

一正向密鑰推導電路，用來依據一母鑰，依序產生該母鑰之複數個後級密鑰至一最後級密鑰為止；

一反向密鑰推導電路，用來依據該最後級密鑰，依序產生該最後級密鑰之複數個前級密鑰至該母鑰為止；以及

至少一位元暫存器，用來儲存該母鑰以及該最後級密鑰；

一加密模組，電連於該密鑰產生模組，用來依據該正向密鑰推導電路所提供之母鑰及依序產生之複數個後級密鑰，依序執行相對應之複數個加密操作，將一明文字串加密為一對應之密文字串；以及

一解密模組，電連於該密鑰產生模組，用來依據該反向密鑰推導電路所提供之最後級密鑰及依序產生之複數個前級密鑰，依序執行相對應之複數個解密操作，將一密文字串解密為一對應之明文字串。

15. 如申請專利範圍第14項之加解密系統，其中該加密模組係為一唯讀記憶體式(ROM-based)加密模組，其包含有複數個唯讀記憶體，用來儲存對應於該複數個加密操作之演算法及相關之應用程式。

16. 如申請專利範圍第14項之加解密系統，其中該明文字串、該密文字串、以及該複數個密鑰皆係為128位元之數位資料。

17. 如申請專利範圍第14項之加解密系統，其中該反向密鑰推導電路包含有：

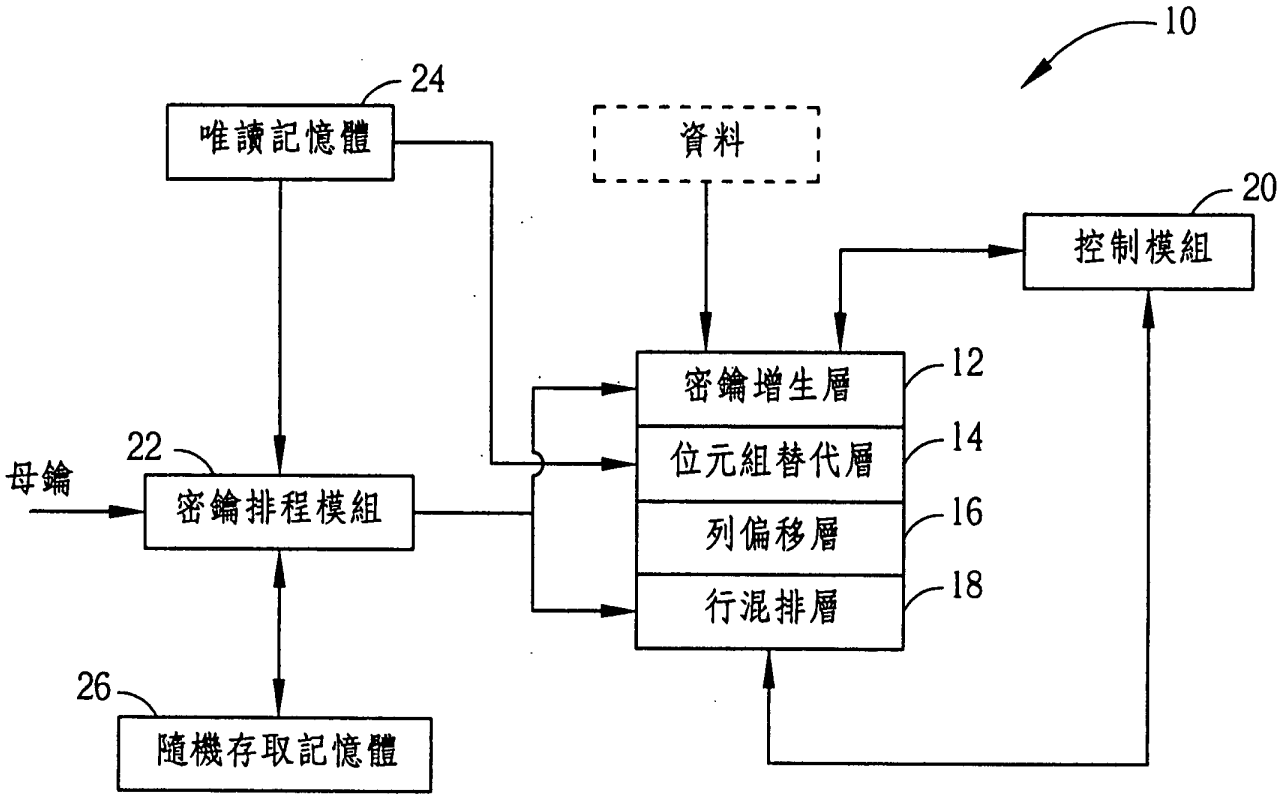
一密鑰接收模組，用來接收該最後級密鑰；

一反向密鑰推導模組，其包含複數個互斥或(XOR)邏輯閘以及一數位資料處理模組，用來將該密鑰接收模組所接收的最後級密鑰經過複數次反向推導處理後，依序產生該最後級密鑰之複數個前級密鑰至該母鑰為止；以及

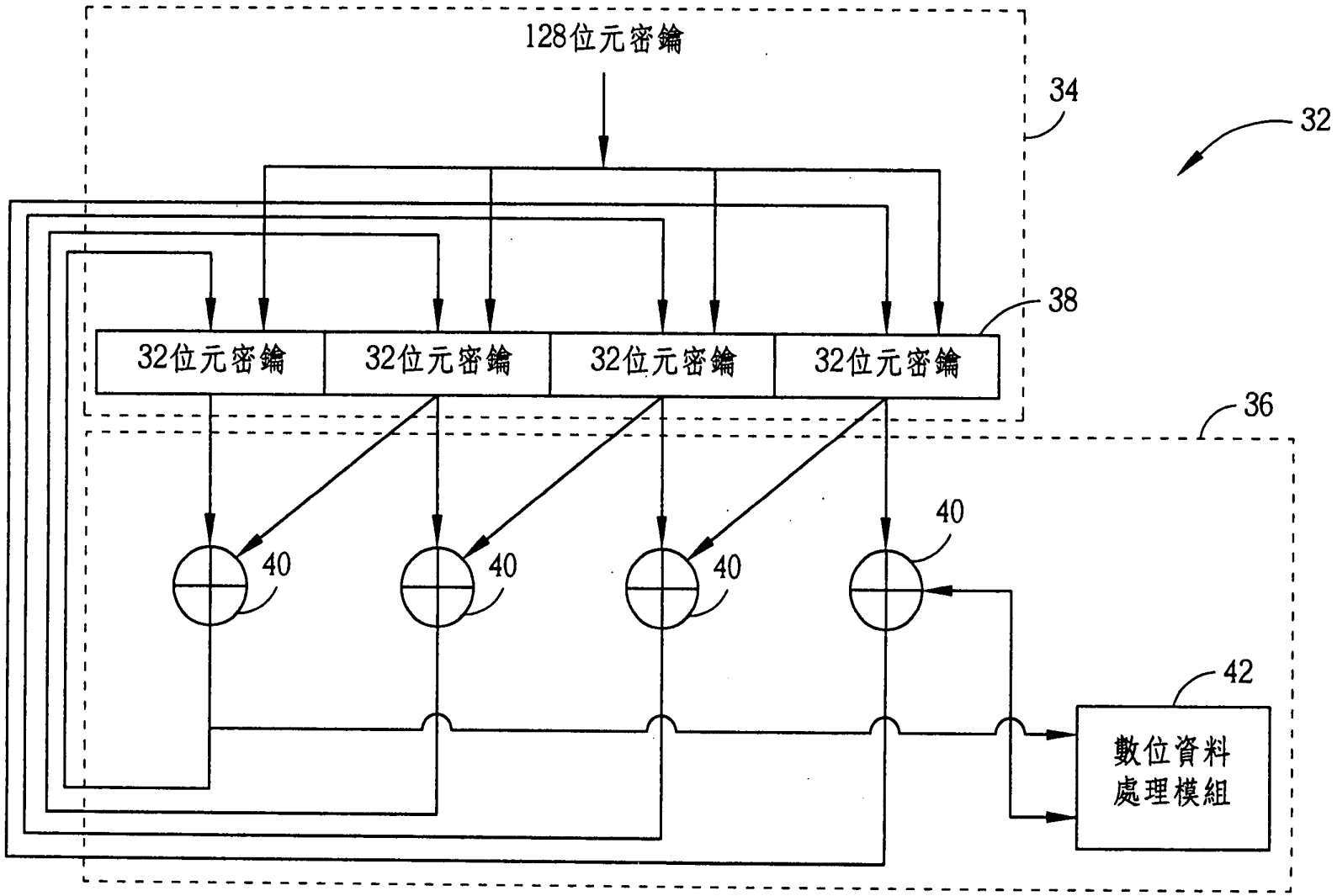
一位元暫存器，電連於該反向密鑰推導模組，用來儲存一經一次該反向推導處理後所得出的密鑰，其中儲存於該位元暫存器之密鑰會被由該密鑰經一次反向推導處理後所產生的前一級密鑰所取代。

18. 如申請專利範圍第14項之加解密系統，其係符合一先進加密標準(Advanced Encryption Standard, AES)，

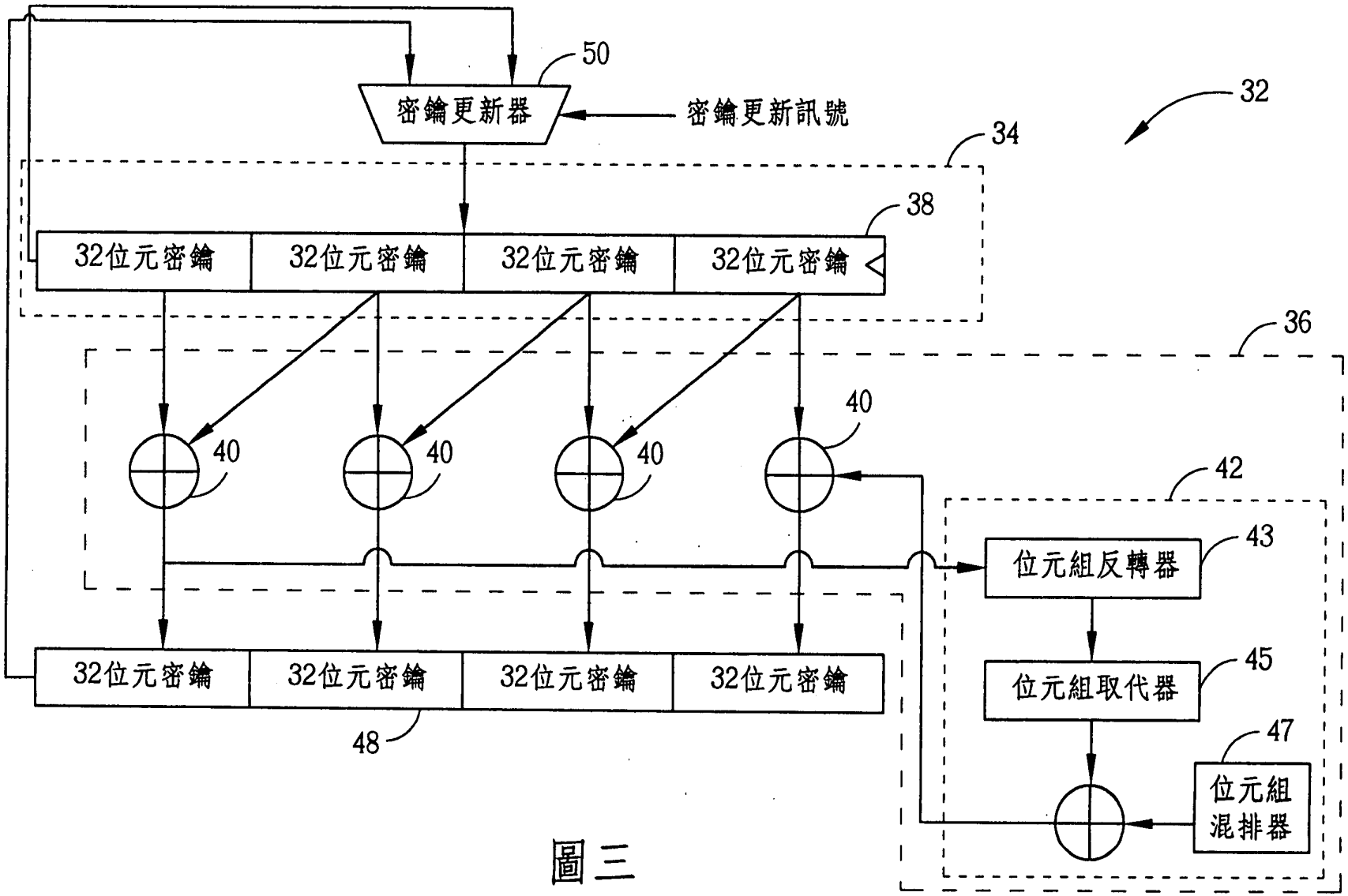
19. 如申請專利範圍第18項之加解密系統，其係應用於一無線區域網路(Wireless LAN)之一加解密系統上。


10
24
唯讀記憶體
資料
20
控制模組
密鑰增生層
12
位元組替代層
14
列偏移層
16
行混排層
18
22
母鑰
密鑰排程模組
26
隨機存取記憶體

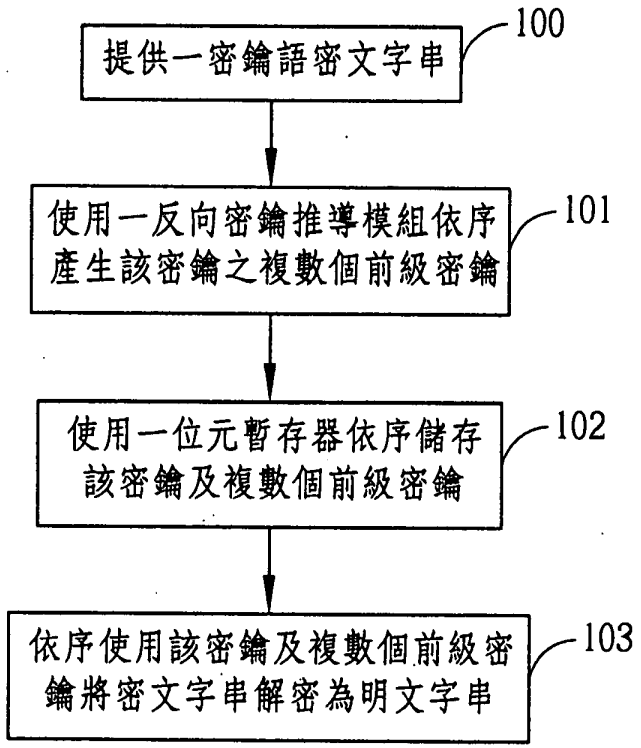
圖一


128位元密鑰
34
32
38
32位元密鑰
32位元密鑰
32位元密鑰
32位元密鑰
36
40
40
40
40
42
數位資料
處理模組

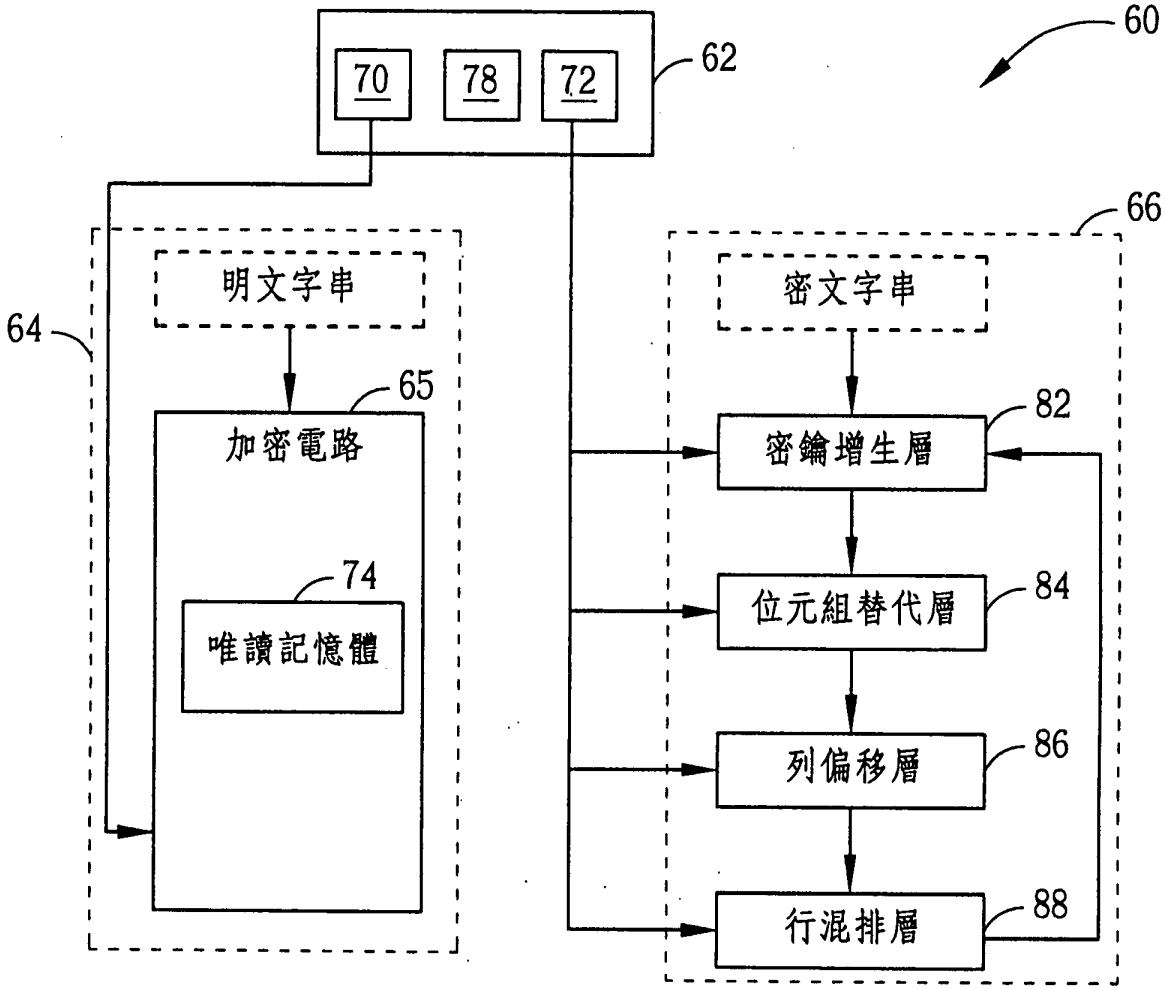
圖二


50
密鑰更新器
密鑰更新訊號
32
34
38
32位元密鑰
32位元密鑰
32位元密鑰
32位元密鑰
36
40
40
40
40
42
位元組反轉器
43
位元組取代器
45
47
位元組
混排器
32位元密鑰
32位元密鑰
32位元密鑰
32位元密鑰
48

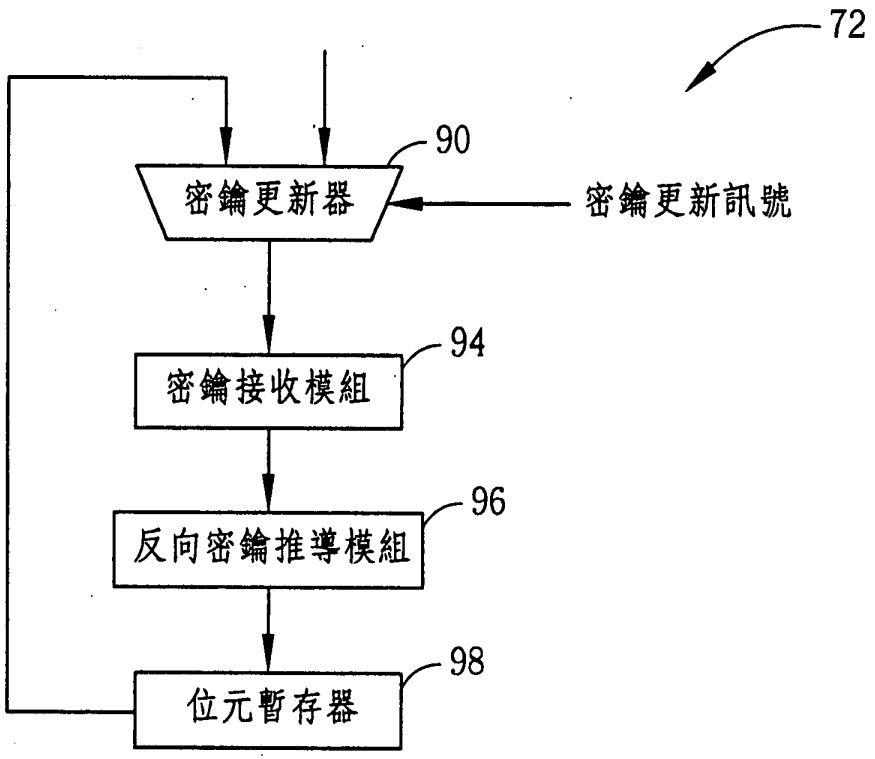
圖三


提供一密鑰語密文字串
100
使用一反向密鑰推導模組依序產生該密鑰之複數個前級密鑰
101
使用一位元暫存器依序儲存該密鑰及複數個前級密鑰
102
依序使用該密鑰及複數個前級密鑰將密文字串解密為明文字串
103

圖四


60
62
70
78
72
66
64
明文字串
密文字串
65
加密電路
82
密鑰增生層
74
唯讀記憶體
84
位元組替代層
86
列偏移層
88
行混排層

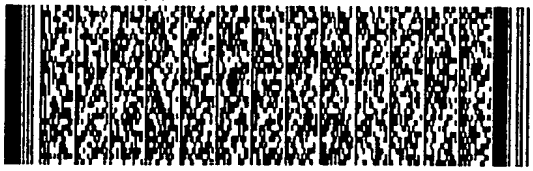
圖五



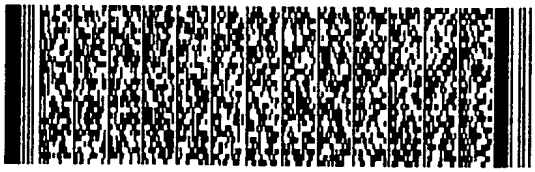
圖六

申請案件名稱:具有一反向密鑰推導電路之加解密系統

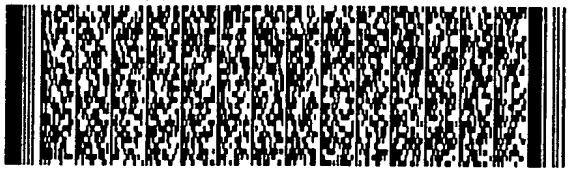
第 1/28 頁



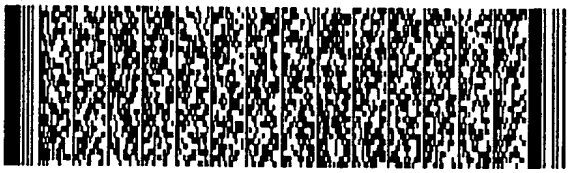
第 1/28 頁



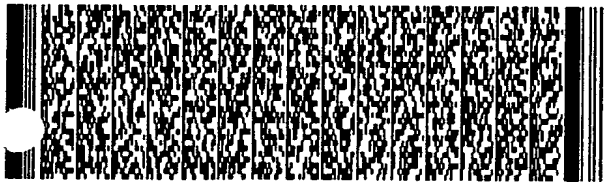
第 2/28 頁



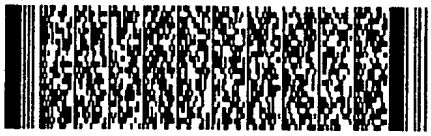
第 2/28 頁



第 3/28 頁

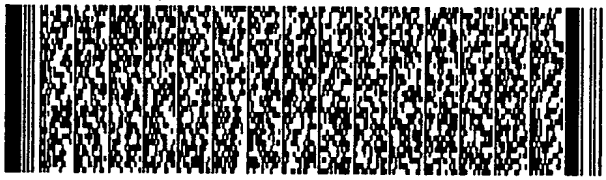


第 4/28 頁

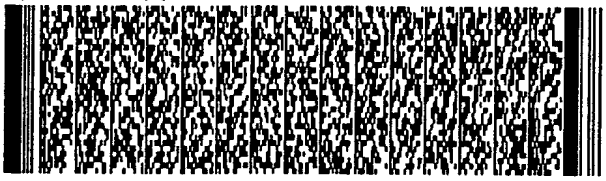


第 5/28 頁

第 6/28 頁

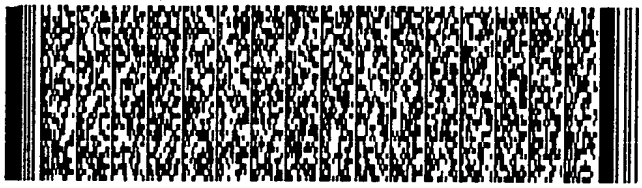


第 6/28 頁

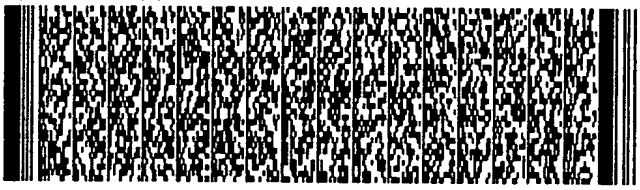


第 7/28 頁

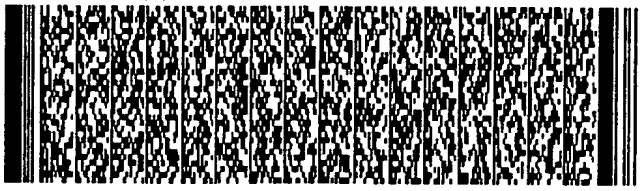
7/28 頁



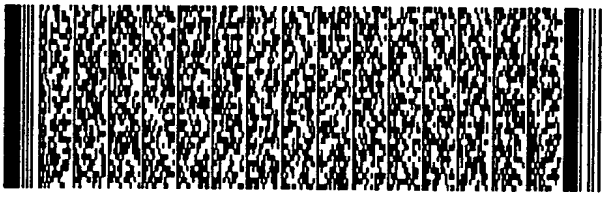
第 8/28 頁



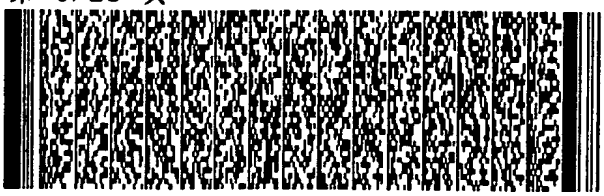
第 8/28 頁



第 9/28 頁

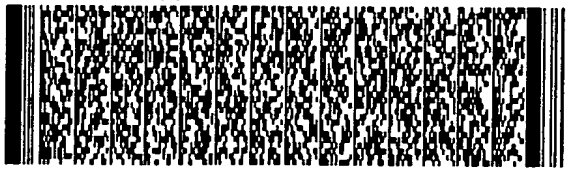


第 9/28 頁

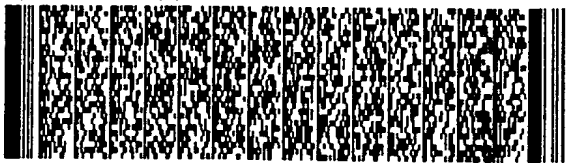


第 10/28 頁

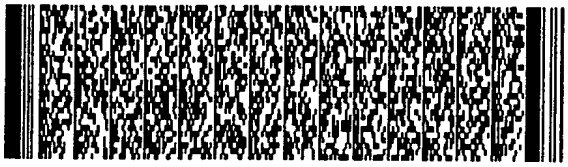
第 10/28 頁



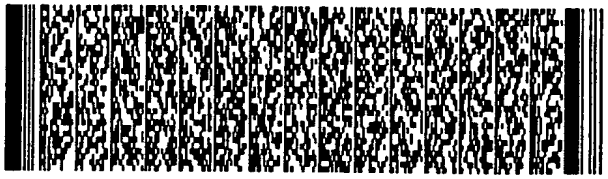
第 11/28 頁



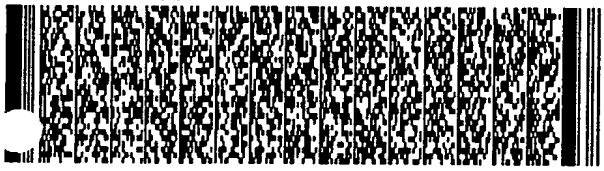
第 11/28 頁



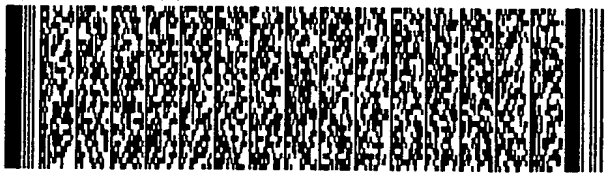
第 12/28 頁



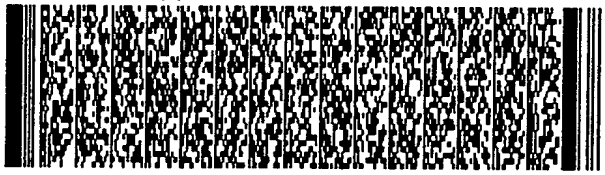
第 12/28 頁



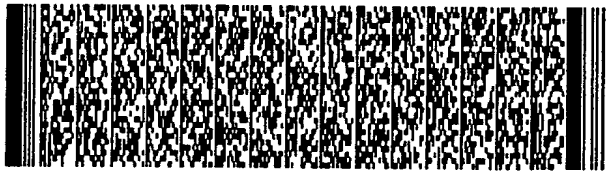
第 13/28 頁



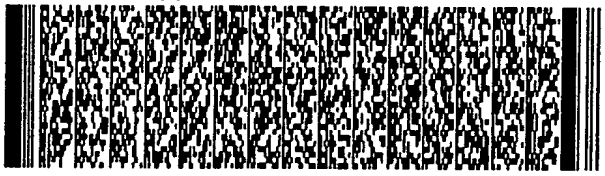
第 13/28 頁



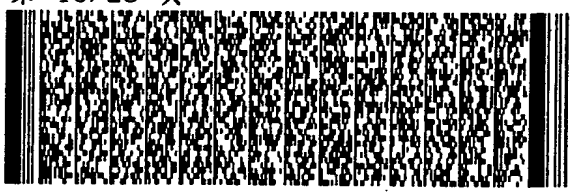
第 14/28 頁



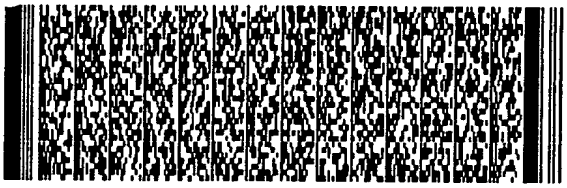
第 14/28 頁



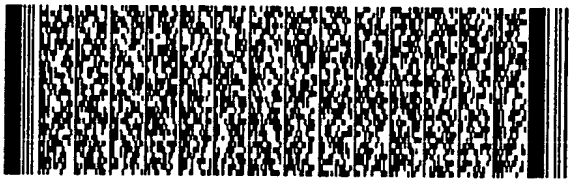
第 15/28 頁



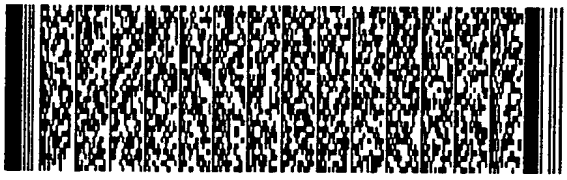
15/28 頁



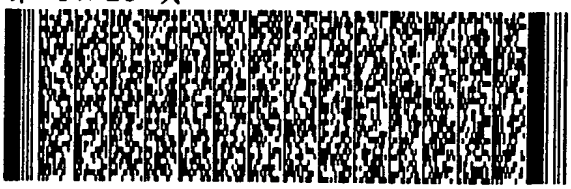
第 16/28 頁



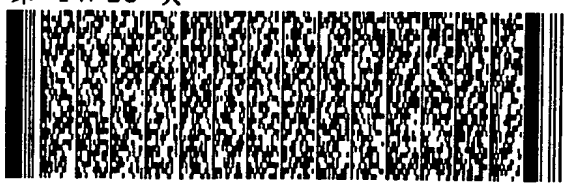
第 16/28 頁



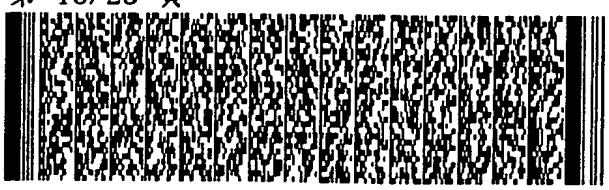
第 17/28 頁



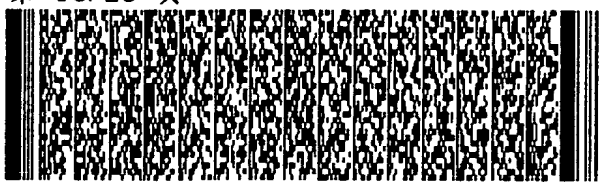
第 17/28 頁



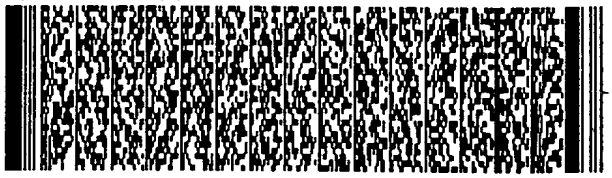
第 18/28 頁



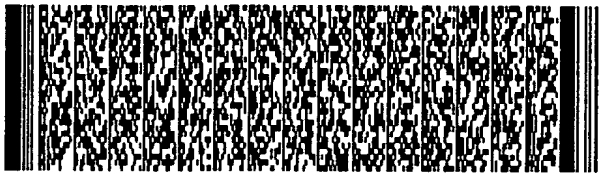
第 18/28 頁



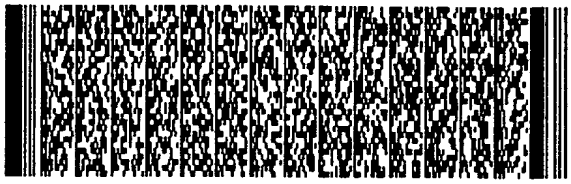
第 19/28 頁



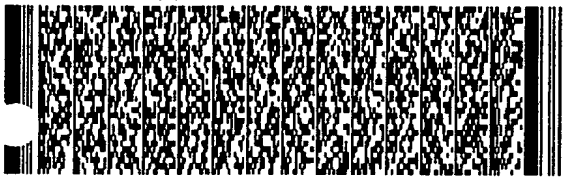
第 19/28 頁



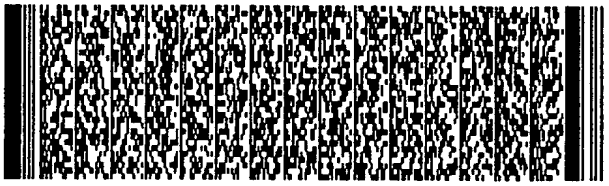
第 20/28 頁



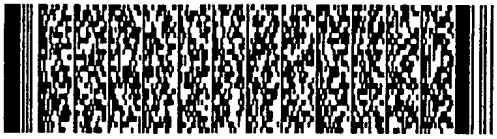
第 20/28 頁



第 21/28 頁



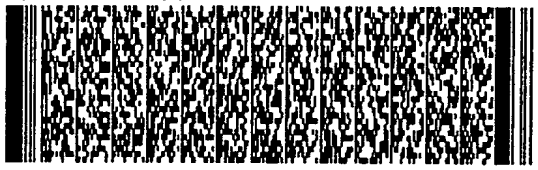
第 22/28 頁



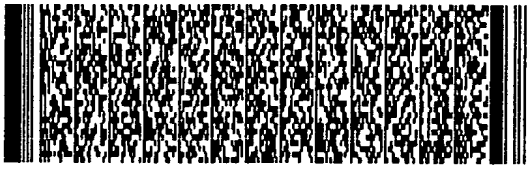
第 23/28 頁

第 23/28 頁

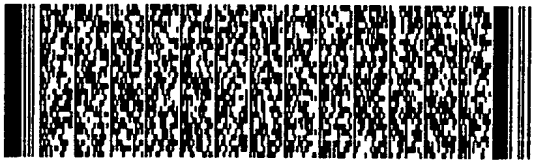
第 24/28 頁



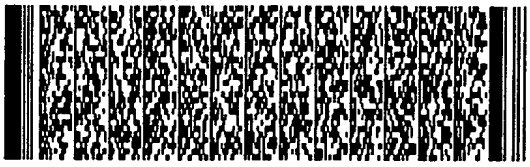
第 24/28 頁



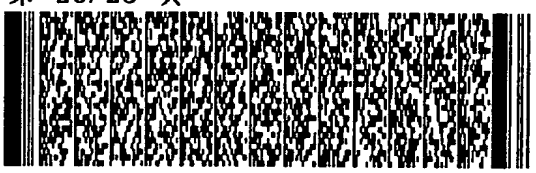
第 25/28 頁



第 25/28 頁



第 26/28 頁



第 26/28 頁

第 27/28 頁